Hands-on tutorials

AWS Security Platform as a Service (PaaS) - Multi-Cloud Security Operations Console

AWS Security Platform as a Service (PaaS) - Multi-Cloud Security Operations Console: Hands-on tutorials

Table of Contents

AWS Security Platform as a Service - Multi-cloud security operations console

AWS experience	Intermediate
Time to complete	2 hours
Cost to complete	See services for specific pricing details.
Services used	Amazon OpenSearch Service, Amazon Security Lake, Amazon GuardDuty, Amazon Inspector, AWS Systems Manager, and AWS Security Hub CSPM
Last updated	January 12, 2026

Overview

This tutorial shows you how to implement a complete AWS Security Platform as a Service (PaaS) that provides a unified security operations console. You'll learn to integrate Cloud Security Posture Management (CSPM), Security Information and Event Management (SIEM), and Cloud Workload Protection Platform (CWPP) capabilities through a single interface with multi-cloud support.

This tutorial focuses on Microsoft Azure and Google Cloud Platform integration, but you can apply the same approach to any cloud provider or on-premises.

What you will accomplish

- Monitor security across multiple cloud providers from a single console
- Detect threats and vulnerabilities in real time
- Maintain compliance posture across your multi-cloud infrastructure
- Respond to security incidents efficiently with centralized analytics

Prerequisites

For this tutorial, you'll need:

- An AWS account with administrator-level access: If you don't already have one, follow the Setting Up Your AWS Environment getting started guide for a quick overview
- Active subscriptions to Microsoft Azure and Google Cloud Platform
- AWS CLI installed
  - See Installing or updating the latest version of the AWS CLI
- Node.js: Version 18.x or later
  - Download from nodejs.org
- AWS CDK: Installed globally
  - Installation command: `npm install -g aws-cdk`
- Security Lake: Preconfigured Amazon Security Lake instance with an Amazon S3 bucket
  - See Getting started with Amazon Security Lake
- AWS Lake Formation: Admin role configured for Security Lake operations
- AWS Identity and Access Management (IAM) permissions: Sufficient permissions to create Lambda functions, SQS queues, KMS keys, and IAM roles

Azure integration requirements:

- Azure Event Hub namespace and connection strings
- Microsoft Defender for Cloud continuous export configured
- Service principal with appropriate permissions

Google Cloud integration requirements:

- Google Cloud Pub/Sub subscription configured
- Service account credentials with Security Command Center permissions
- Organization-level or project-level access